WE CLAIM:

1. A method for tracing content in a highly distributed system, comprising:

receiving content associated with a content owner;

decrypting the received content;

associating a first set of information with the decrypted content, wherein the first set of information, in part, uniquely identifies an entity decrypting the content; and

providing a second set of information to the content owner, wherein the second set of information enables the content owner to trace the content in the highly distributed system.

2. The method of claim 1, wherein decrypting the received content further comprises:

obtaining an access key out-of-band, wherein the access key is uniquely associated with the entity decrypting the content and a sender of the content; and

employing the access key to unwrap the received content.

3. The method of claim 1, wherein associating the first set of information further comprises:

determining a self-identifier associated with the entity decrypting the content;

determining a fingerprint based, in part, on the self-identifier; and

watermarking the decrypted content employing the fingerprint.

4. The method of claim 3, wherein the self-identifier is digitally signed by an encryption key associated with the entity decrypting the content.

5. The method of claim 3, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted.

6. The method of claim 1, wherein the second set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the entity decrypting the content.

7. The method of claim 1, further comprising:

determining a self-identifier associated with the entity decrypting the content;

determining an access key associated with another recipient of the content and the entity;

encrypting the content;

wrapping the encrypted content and the self-identifier employing the access key;

forwarding the wrapped and encrypted content to the other recipient.

8. The method of claim 7, wherein determining the access key further comprises receiving the access key employing an out-of-band mechanism.

9. The method of claim 7, wherein wrapping the encrypted content further comprises digitally signing the encrypted content.

10. The method of claim 7, wherein the access key employs a public key infrastructure.

11. The method of claim 1, wherein the content is at least one of a subscription television, movies, interactive video games, video conferencing, audio, still images, text, graphics.

12. A security device for tracing content in a highly distributed system, comprising:

a receiver configured to receive content associated with a content owner;

a fingerprinter-watermarker configured to perform actions including:

determining a self-identifier that uniquely identifies a recipient of the content;

determining a fingerprint based, in part, on the self-identifier; and

watermarking the content employing the fingerprint; and

a forensics interface configured to send information associated with the watermarked content to the content owner.

13. The security device of Claim 12, further comprising:

a key wrap, coupled to the fingerprinter-watermarker, that is configured to perform actions, including:

receiving an access key associated with the recipient of the content; and

wrapping the content and the self identifier employing the access key.

14. The security device of claim 13, wherein the access key is received employing an out-of-band mechanism.

15. The security device of claim 12, wherein the recipient is at least one of an aggregator, a service operator, and a user.

16. The security device of claim 12, wherein the information associated with the watermarked content comprises at least one of traceability information, a time stamp,

an identifier, and registration information associated with at least one of the content and the recipient of the content.

17. The security device of claim 12, further comprising:

a data store configured to store decrypted content; and

a fingerprinted-watermarked content data store configured to store encrypted content.

18. A modulated data signal having computer executable instructions embodied thereon for delivering content in a highly distributed system, the modulated data signal comprising actions including:

transferring content from a market participant to another market participant;

enabling a decryption of the content, if the transferred content is encrypted;

enabling an association of information with the decrypted content, wherein the information uniquely identifies an entity associated with the decryption of the content; and

providing the information concerning the decrypted content to the content owner.

19. The modulated data signal of claim 18, wherein information associated with the content further comprises at least one of a fingerprint, a watermark, a time stamp, and a serial number.

20. An apparatus for tracing content in a highly distributed system, comprising:

a means for receiving content associated with a content owner;

a decryption means for decrypting the received content;

a means for associating a first set of information with the decrypted content, wherein the first set of information, in part, uniquely identifies an entity decrypting the content;

a means for determining a second set of information associated with the decryption of the content; and

a means for providing the second set of information to the content owner.